UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/777,305	02/13/2004	In-Zoo Lee	P56955	5304

7590 07/18/2007

Robert E. Bushnell
Suite 300
1522 K Street, N.W.
Washington, DC 20005-1202

EXAMINER	
HAILU, TESHOME	
ART UNIT	PAPER NUMBER
2109	
MAIL DATE	DELIVERY MODE
07/18/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/777,305	LEE, IN-ZOO	
	Examiner	Art Unit	
	Teshome Hailu	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *13 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *02/13/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-10 are pending.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-10 are rejected under 35 U.S.C. 102(e) as being anticipated by Lantto et al (Lantto), US Pub. No. 2004/0054794.

As per claim 1, Lantto discloses:

- A method for **encrypting data** in an access **virtual private network (VPN)**, comprising the steps of: (Page 7, paragraph 164, "The ***VPN software*** will then perform the necessary step to establish the secure connection by ***negotiating bulk encryption keys with the VPN gateway 415***").

- performing a **link control protocol (LCP) negotiation** regarding at **least one of an authentication method**, data compression, maximum data size receivable, link status monitoring, and whether to perform data encryption; (Page 6, paragraph 143, "***PPP Link Control Protocol (LCP)***: the

computer 401 and the GPRS device 403 ***exchange several messages to negotiate link parameters*** e.g. Maximum Receive Unit (MRU), ***Authentication Protocol***.")

- checking a **user identification (ID) and a password when the LCP negotiation determines** that mutual authentication is required, said negotiation being conducted by two terminals according to an LCP negotiation condition at the step of performing the LCP negotiation; (Page 6, paragraph 143, "***PPP Link Control Protocol (LCP)***: the computer 401 and the GPRS device 403 ***exchange several messages to negotiate link parameters*** e.g. Maximum Receive Unit (MRU), ***Authentication Protocol***"). Moreover, (page 2, paragraph 32, "***Authentication***: ***These are techniques that enable to ensure that both ends of the session, the user and the remote network access server, are really who they say they are***. This is achieved in a number of ways, but generally requires the user to provide some input, e.g. a ***password, a smart card etc***.")

- performing **data encryption** when the step of performing the LCP negotiation results in a determination that **data encryption is to be performed**; (page 2, paragraph 33, "***Encryption***: ***Using a previously agreed encryption algorithm***, machines can scramble the data they exchange so that they can detect any attempt to tamper with it, and ***ensure end-to-end confidentiality***.")

- performing **network control protocol (NCP)** negotiation in order to negotiate information for a Layer 3 **communication access between a user and a private network**; (Page 6, paragraph 145, PPP ***Network Control Protocol (NCP)/IP control protocol (IPCP):*** the RAS request certain IP network parameters (as per the requirements passed by the RAL system) in a 'PPP IPCP configuration request' message. These parameters comprise e.g. ***IP address allocation policy, name servers, end-to-end compression, etc***.")

- **transmitting and receiving data** by forming a session between the **user and the private network** when the **NCP negotiation is performed between the user and the private network**. (Page

2, paragraph 35, "To achieve this, a so-called ***'tunneling protocol'*** is required. ***This protocol gives the illusion that a remote computer 102 us directly connected to the private network 101***. It avoids local machines sending data in clear via an un-secure public gateway 104 when they reply to a remote computer"). Where tunneling protocol is a network protocol.

As per claim 2, Lantto discloses:

- The method according to claim 1, wherein the **NCP negotiation is performed after the data encryption is performed.** (Page 2, paragraph 35, "Instead data to the remote computer is intercepted by the secure gateway 103, e.g. using proxy Address Resolution Protocol (ARP), ***optionally encrypted***, ***then 'encapsulated', and finally routed via the internet 105 to the remote computer 102.")***

As per claim 3, Lantto discloses:

- The method according to claim 1, wherein the NCP negotiation is performed when it is determined, during performance of the LCP negotiation, that **authentication and data encryption are not required**. (Page 2, paragraph 35, "Instead data to the remote computer is intercepted by the secure gateway 103, e.g. using proxy Address Resolution Protocol (ARP), ***optionally encrypted***, then 'encapsulated', and finally routed via the internet 105 to the remote computer 102"). Lantto also disclose, (page 6, paragraph 144, PPP Authentication: Optionally, the RAS component 215 n the computer 401 retrieves the authentication credentials from RAM and pass them on to the GPRS phone 403.

As per claim 4, Lantto discloses:

- The method according to claim 1, wherein an item for selecting whether to **perform data encryption is added to an LCP negotiation option table of the user and the private network** in advance of the step of performing the LCP negotiation. (Page 6, paragraph 143, "PPP Link Control Protocol (LCP): the computer 401 and the GPRS device 403 exchange several messages to negotiate link parameters e.g. Maximum Receive Unit (MRU), Authentication Protocol"). In addition, Lantto disclose,

(Page 7, paragraph 164, "The ***VPN software*** will then perform the necessary step to establish the ***secure connection by negotiating bulk encryption keys with the VPN gateway 415***").

As per claim 5, Lantto discloses:

- The method according to claim 1, wherein the step of **checking the user ID and the password comprises using a password authentication protocol (PAP)** for providing **user authentication by delivering the user ID and the password in form of a text**. (page 2, paragraph 32, "***Authentication***: These are techniques that enable to ensure that both ends of the session, the user and the remote network access server, are really who they say they are. This is achieved in a number of ways, but generally requires the ***user to provide some input, e.g. a password, a smart card etc***, and the machines to perform some cryptographic treatment, e.g. hash functions. ***Password Authentication protocol (PAP)***, Challenge Handshake Authentication Protocol (CHAP) are ***example of standard authentication techniques*** that exists").

As per claim 6, Lantto discloses:

- The method according to claim 1, wherein the step of **checking the user ID and the password comprises using a challenge handshake authentication protocol (CHAP)** for providing ***user authentication using a hash function***. (page 2, paragraph 32, "***Authentication***: These are techniques that enable to ensure that both ends of the session, the user and the remote network access server, are really who they say they are. This is achieved in a number of ways, but generally requires the ***user to provide some input, e.g. a password, a smart card etc***, and the ***machines to perform some cryptographic treatment, e.g. hash functions***. Password Authentication protocol (PAP), ***Challenge Handshake Authentication Protocol (CHAP)*** are ***example of standard authentication techniques*** that exists").

As per claim 7, Lantto discloses:

- The method according to claim 1, wherein the step of performing **data encryption comprises using a data encryption standard (DES)**. (Page 2, paragraph 33, "There is a ***number of encryption algorithms such as Data Encryption Standard (DES)***, 3-DES etc.")

As per claim 8, Lantto discloses:

- The method according to claim 1, wherein the step of performing data **encryption comprises using a user password as a key value for encryption.** (page 2, paragraph 33, "***Encryption: Using a previously agreed encryption algorithm***, machines can scramble the data they exchange so that they can detect any attempt to tamper with it, and ensure end-to-end confidentiality. This however generally requires the two machines to have an identical set of ***cryptographic material or keys*** to seed the encryption algorithm"). According to Lantto, "cryptographic material or key", inherently indicate a password.

As per claim 9, Lantto discloses:

- The method according to claim 1, wherein the LCP negotiation is **performed with respect to both the authentication method and whether to perform data encryption**. (Page 6, paragraph 143, "***PPP Link Control Protocol (LCP)***: the computer 401 and the GPRS device 403 ***exchange several messages to negotiate link parameters*** e.g. Maximum Receive Unit (MRU), ***Authentication Protocol***"). According to Lantto, (page 2, paragraphs 31, 32, 33 and 34, ***Secure networking covers three areas: Authentication, Encryption and Tunnelling or Virtual private Networks (VPNs)***)

As per claim 10, Lantto discloses:

- The method according to claim 9, wherein the step of **performing data encryption comprises using a user password as a key value for encryption**. (page 2, paragraph 33, "**Encryption: Using a previously agreed encryption algorithm, machines can scramble the data they exchange** so that they can detect any attempt to tamper with it, and ensure end-to-end confidentiality. This however generally requires the ***two machines to have an identical set of cryptographic material or keys to***

seed the encryption algorithm"). According to Lantto, "cryptographic material or key", inherently indicate a password.

Conclusion

4. The prior art made or record and not relied upon is considered pertinent to applicant' s disclosure.

TITLE: Appartus and method for performing and controlling encryption/decryption for data to be transmitted on local area network, US 6,275,588.

TITLE: Automatic discovery of network core type, US Pub. No. 2004/0052257.

TITLE: Method and system for enabling layer 2 transmission of IP data frame between user terminal and service provider, US Pub. No. 2003/0037163.

TITLE: Method and arrangement to secure access to a communication network, US 7,152,160.

TITLE: Mobile virtual network system and method, US 6,970,459.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Teshome Hailu whose telephone number is (571) 270-3159. The examiner can normally be reached on Mon-Fri 7:30a.m. to 5:00p.m. PST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Chamili Das can be reached on (571) 272-3696. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Teshome Hailu

TH

Patent Examiner

Chameli Das

***

CHAMELI DAS
SUPERVISORY PATENT EXAMINER

7/6/07.